AMENDMENTS TO THE SPECIFICATION:

(1) Please amend the paragraph on page 1, lines 6-11, as follows:

The invention relates to network selection procedures for communication networks, e.g., ~~IP~~ Internet Protocol (IP) networks such as wired and wireless local area networks (LANs). More specifically, the invention relates to arrangements wherein a plurality of network operators share an IP network.

(2) Please amend the paragraph beginning on page 2, line 29, and ending on page 3, line 12, as follows:

During authentication of clients requesting access to the network AN, the access service provider ASP will send an authentication request to one of the service providers directly connected thereto, namely VSP1, VSP2, VSP3 or HSPC. In fact the access service provider ASP is not in a position to authenticate users A and B locally. In current arrangements, the access service provider ASP will take the corresponding decisions in an autonomous way, without receiving from the users A or B any input data other than their identity. Such a situation may explain why network advertising, i.e., the announcement of network operators available in a given public WLAN and the need for network selection are described in documents such as 3GPP S2-031899 "WLAN Network selection", San Diego Meeting, 12-16 May 2003 ~~(www.3gpp.org/ftp/tsg_sa/WG2_Arch/TSGS2_32_San_Diego/tdocs)~~, while indicating that the mechanism for network advertising is still "to be discussed".

(3) Please amend the paragraph on page 3, lines 13-21, as follows:

An alternative arrangement based on XML meta-language has been proposed by document 3GPP S2-031864 "Network Selection", San Diego Meeting, 12-16 May 2003 ~~(www. 3gpp.org/ftp/tsg_saWG2_Arch/TSGS2_32_San_Diego/tdocs)~~. The corresponding arrangement has the disadvantage of requiring XML pre-configuration. Furthermore, the XML code has an increased amount of tagging information, which requires a greater amount of bits to be transmitted.

(4) Please amend the paragraph beginning on page 3, line 30, and ending on page 4, line 4, as follows:

The present invention also relates to a corresponding communication network and a computer program product loadable in the memory of at least one computer and including software code portions for performing the method of the invention. Reference to at least one computer is evidently intended to take into account that the method of the invention is adapted to be carried out in a ~~decentralised~~ decentralized manner, with different tasks being allotted to different computers in a network.

(5) Please amend the paragraph on page 4, lines 15-20, as follows:

This arrangement is independent from [[of]] the access technology deployed within the access network. This can be either wireless (e.g., a WLAN network) or wired (e.g., a PSTN network with dial-up access). For the sake of simplicity, a wireless LAN will be steadily referred to in the following as a preferred example.

(6) Please amend the paragraph beginning on page 4, line 28, and ending on page 5, line 8, as follows:

A preferred embodiment of the arrangement described herein is based on the so-called Diameter agent supported in a Diameter base protocol. The basic related information is provided, e.g., in IETF draft-ietf-aaa-diameter-17.txt, "Diameter Base Protocol", ~~www.ietf.org~~. The Diameter agent is used to provide an authentication, authorization and accounting (AAA) framework for applications such as network access or IP mobility. Essentially, a Diameter agent is a Diameter node that provides either relay, proxy, redirect or translation services. Specifically, the arrangement described herein provides for certain modifications being made in the way specific Diameter requests are processed and the relative answers are created by the Diameter agent when these authentication requests have an unknown realm.

(7) Please amend the paragraph on page 5, lines 17-25, as follows:

Those of ordinary skill in the art will appreciate that the same arrangement could also be used with other "triple-A" protocols such as, e.g., the protocol currently referred to as Remote Authentication Dial-In User Service (RADIUS): this does not provide for explicit support for agents, including so-called proxies, redirects and relays. The expected ~~behaviour~~ behavior will not be defined, as this may vary for different implementations.

(8) Please amend the paragraph on page 5, lines 26-35, as follows:

The list of supported visited networks having a roaming agreement with a certain user's "home" ISPs are sent to the user by the authentication server of the provider

acting as the access provider. This preferably occurs during the user authentication procedure, using an extensible authentication protocol (EAP). This authentication protocol (as described, e.g., in IETF draft-ietf-eap-rfc2284bis-03.txt, ~~www.ietf.org~~) supports multiple authentication mechanisms and typically runs directly over the link.

(9) Please amend the paragraph on page 6, lines 1-7, as follows:

For this purpose, a modification to the EAP procedure is advisable that consists in adding two messages to the normal sequence of packets exchanged during the authentication. However, the method proposed should be supported by a generic authentication mechanism ~~indipendently~~ independently of the underlying WLAN standard.

(10) Please delete the paragraphs beginning on page 6, line 13, and ending on page 8, line 2, as follows:

~~In a presently preferred embodiment of the invention, the user is identified univocally by means of an identifier.~~

~~This may be e.g. the network access identifier known as NAI described e.g. in RFC 2486 3GPP S2-031864 "Network selection", San Diego Meeting, 12-16 May 2003 (www.3gpp.org/ftp/tsg_sa/WG2_Arch/TSGS2_32_San_Diego/tdocs).~~

~~In such a preferred embodiment, the user sends his or her credentials to the access network (which may occur by means of either a wired device or a wireless device). The access network forwards these credentials to a back-end authentication server, located at the data center of the access service provider. The authentication server retrieves the available roaming networks for that user, identified through the~~

realm part of the NAI. To accomplish this task, the server initiates a conversation with the servers belonging to the providers to which it is connected. As a result, the authentication server retrieves the list of operators that hold a roaming agreement with the user's operator(s). This procedure is performed only once when a first authentication request is received by the authentication server in respect of a user for which no direct roaming agreements exist with the home server provider of such a user. The authentication server also forwards, via the access network, a list of operators to the user. The user chooses one of the operators from the list received from the server, according to his or her preferences, or based on some pre-configured settings. When presented with such a list, the user will send the chosen operator identifier back to the authentication server in the access network and the authentication server will forward to the provider chosen by the user the authentication request, containing the user's credentials.

Of course, in the case the provider acting as the access provider has a direct roaming agreement with the user's home service provider, the user will be presented with a list comprised of one operator only. Alternatively, under these circumstances, the authentication server may simply decide to directly forward the authentication request to the user's home service provider.

The user will then perform a usual authentication procedure with his service provider (for example, using a standard mechanism like EAP). While performing the steps of this procedure, the authentication information flows through the network of the previously chosen operator. Specifically, the authentication server will forward authentication messages to the visited authentication server. These will in turn proxy such messages to the home operator server, i. e. the home authentication server.

~~Being given the possibility of choosing the provider to which the access service provider will forward the authentication request, the users will in fact route their data flows with the ensuing possibility of making choices e. g. in terms of pricing and quality of service (QoS) granted.~~

(11) Please amend the paragraph on page 8, lines 14-16, as follows:

- figure 4 is a functional block diagram schematically representing a ~~generalised~~ generalized network selection procedure,

(12) Please amend the paragraph on page 9, lines 7-9, as follows:

It will be assumed that a 3G subscriber wishes to ~~utilise~~ utilize the resources and access to services within the respective own 3GPP operator network.

(13) Please amend the paragraph on page 10, lines 7-15, as follows:

The arrangement described is intended to give the user the possibility of selecting a ~~signalling~~ signaling path to obtain authentication and authorization from the home network. Any subsequent user data flow will in fact be highly likely to follow the same path used for ~~signalling~~ signaling. The possibility thus exist for the user of making choices between different commercial agreements, e.g., in terms of pricing and quality of service (QoS) granted.

(14) Please amend the paragraph on page 10, lines 22-35, as follows:

This applies, e.g., to the IEEE 802.11 standard, but similar remarks apply to other WLAN technologies. In fact, in the case of IEEE 802.11 WLANs, the WLAN

network name is conveyed over the WLAN beacon signal in the so-called SSID (Service Set ID) information element. The possibility also exists for a user equipment (UE) to actively solicit support for specific SSIDs by sending a probe request message and by receiving a reply if the access point does support the solicited ~~SSIDas~~ SSIDs defined by IEEE 802.11. However, in such prior art arrangements the user will not become aware of the set of supported visited networks and thus ~~possbily~~ possibly select the path for reaching the desired home operator by using this mechanism.

(15) Please amend the paragraph on page 11, lines 9-24, as follows:

In the case of WLAN-3G system interworking, support in that respect can be provided by a generic authentication mechanism (~~indipendently~~ independently of the underlying WLAN standard), such as, e.g., the extensible authentication protocol currently referred to as EAP. In the case of 3G users the authentication mechanism to be transported may thus be based, e.g., on the existing EAP/AKA authentication mechanism described in the Internet Draft "draft-arkko-pppext-eap-aka-09.txt", "EAP AKA Authentication", February 2003, ~~www.ietf.org/internet-drafts/draft-arkko-pppext-eap-aka-09~~. An alternative may be represented by the EAP/SIM authentication mechanism described in the Internet Draft "draft-haverinen-pppext-eap-sim-10.txt", "EAP SIM Authentication", February 2003, ~~www.ietf.org/internet-drafts/draft-haverinen-pppext-eap-sim-lOtxt~~.

(16) Please insert the following paragraphs after page 12, line 8, as follows:

In a presently preferred embodiment of the invention, the user is identified univocally by means of an identifier.

This may be, e.g., the network access identifier known as NAI described, e.g., in RFC 2486 3GPP S2-031864 "Network selection", San Diego Meeting, 12-16 May 2003.

In such a preferred embodiment, which is illustrated in Fig. 4, the user sends his or her credentials to the access network (which may occur by means of either a wired device or a wireless device) via an AN (Fig. 4, Step 1 and Step 2). The access network forwards these credentials to a back-end authentication server, located at the data center of the access service provider. The authentication server retrieves the available roaming networks for that user, identified through the realm part of the NAI. To accomplish this task, the server initiates a conversation with the servers belonging to the providers to which it is connected (Fig. 4, Step 3). As a result, the authentication server retrieves the list of operators that hold a roaming agreement with the user's operator(s) (Fig. 4, Step 4). This procedure is performed only once when a first authentication request is received by the authentication server in respect of a user for which no direct roaming agreements exist with the home server provider of such a user. The authentication server also forwards, via the access network, a list of operators to the user (Fig. 4, Step 5). The user chooses one of the operators from the list received from the server, according to his or her preferences, or based on some pre-configured settings. When presented with such a list, the user will send the chosen operator identifier back to the authentication server in the access network (Fig. 4, Step 6). The authentication server will forward to the provider chosen by the user the authentication request, containing the user's credentials (Fig. 4, Step 7).

Of course, in the case the provider acting as the access provider has a direct roaming agreement with the user's home service provider, the user will be presented with a list comprised of one operator only. Alternatively, under these circumstances, the

authentication server may simply decide to directly forward the authentication request to the user's home service provider.

The user will then perform a usual authentication procedure with his service provider (for example, using a standard mechanism like EAP). While performing the steps of this procedure, the authentication information flows through the network of the previously chosen operator. Specifically, the authentication server will forward authentication messages to the visited authentication server. These will in turn proxy such messages to the home operator server, i.e., the home authentication server (Fig. 4, Step 8). Being given the possibility of choosing the provider to which the access service provider will forward the authentication request, the users will in fact route their data flows with the ensuing possibility of making choices, e.g., in terms of pricing and quality of service (QoS) granted.

(17) Please amend the paragraph on page 12, lines 11-15, as follows:

As a first step, the access network device sends an EAP-request/identity message to the user equipment (UE) for user's credentials. EAP packets are transported over the wireless LAN interface encapsulated within any wireless LAN ~~tecnology~~ technology specific protocol.

(18) Please amend the paragraph on page 15, lines 16-22, as follows:

As shown in figure 6, if the AauS receives all the redirect notifications with the redirect host AVP = unknown, then it forwards the authentication request, as received in the third step above, to the ~~Vaus spedified~~ VauS specified in the default entry of its

routing table. This operation will be carried out only after the reception of the unsuccessful notifications.

(19) Please amend the paragraph on page 18, line 20, as follows:

The procedure for web-based user authentication, which is illustrated in Fig. 7, is described below.

(20) Please amend the paragraph on page 18, lines 21-26, as follows:

The User A requests a service from a wireless internet service provider ISP, e.g., by "opening" a web browser and by subsequently requesting a URL (Fig. 7, Step 1). The access network device intercepts the user's request and in turn asks the user for his or her credentials, via a HTML page (Fig. 7, Step 1).

(21) Please amend the paragraph beginning on page 18, line 27, and ending on page 19, line 3, as follows:

The user A submits his or her identity (e.g., in NAI format) and password. The credentials are transported to the access network device using HTTPS (Fig. 7, Step 2). The access network device forwards them to the access authentication server (AauS) using Diameter encapsulation (Fig. 7, Step 2). The access authentication server (AauS) in the WISP retrieves the available roaming networks for that user. These are identified through the realm part of the NAI identifier. To accomplish this task, the server initiates a conversation with all the servers belonging to the providers to which it is connected to, as described previously (Fig. 7, Step 3).

(22) Please amend the paragraph on page 19, lines 4-7, as follows:

As a result, the authentication server retrieves the list of operators that hold a roaming agreement with the user's operator (Fig. 7, Step 4). The access authentication server (AauS) sends this list of operators to the user (Fig. 7, Step 5).

(23) Please amend the paragraph on page 19, lines 14-17, as follows:

The list is presented to the user with a new HTML page with IP network selection links. The user chooses one of the operators included in the list received from the server, and the selection is then electronically sent back to the ASP via the AN (Fig. 7, Step 6).

(24) Please amend the paragraph on page 19, lines 18-25, as follows:

At this point, the authentication server forwards the authentication request, containing the user credentials, to the provider chosen by the user (Fig. 7, Step 7). The home authentication server accepts the user credential, checks the user's identity for validation and if authentication is successful, orders to the access authentication server to give the user service (Fig. 7, Step 8). ~~The corresponding procedure is depicted in figure 7.~~